Informationssäkerhet

- Ledningens genomgång år 2024

Kungsholmens stadsdelsförvaltning

Ledningens genomgång
Bilaga till Verksamhetsplan 2024
Dnr: KUNG 2023/464
Kontaktperson: Frida Mattsson

Ledningens genomgång är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare samt om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan.

Innehållsförteckning

1 Riktlinje för informationssäkerhet

Kommunfullmäktige har fastställt riktlinjerna för informationssäkerhet i staden. Riktlinjerna består dels av övergripande mål och principer för informationssäkerhetsarbetet och dels av följande sju fördjupade tillämpningsanvisningar:

1. Ansvar och roller inom informationssäkerhet
2. Kartläggning och klassning av information
3. Identitet och åtkomst
4. Anskaffning och utveckling av varor och tjänster
5. Drift och förvaltning av IT-tjänster
6. Incidenthantering och kontinuitetshantering
7. Loggning och spårbarhet.

Riktlinjen och tillämpningsanvisningarna ska tillämpas i arbetet med informationssäkerhet inom samtliga nämnder och bolagsstyrelser i Stockholms stad. Riktlinjen och tillämpningsanvisningarna ska även tillämpas i arbetet med dataskydd som följer av dataskyddslagstiftningen, det vill säga dessa krav samordnas inom ramen för samma styrdokument.

1.1 Lokal anvisning för informationssäkerhet

Förvaltningschef har för nämndens räkning under 2023 fastställt en lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. Den lokala anvisningen ska implementeras under 2024.

1.2 Verksamhetsplan

Aktiviteter som rör informationssäkerhet och dataskydd är implementerat i verksamhetsplan och arbetet med intern kontroll. I verksamhetsplan fastställs de aktiviteter, risker, kontroller och eventuella åtgärder som ligger till grund för informationssäkerhetsarbetet nästkommande år.

2 Uppföljning informationssäkerhetsarbete och dataskyddsarbete

Förvaltningens årshjul för informationssäkerhet följer arbetet med verksamhetsplan och de aktiviteter som fastställts, samt kontroller och eventuella åtgärder som identifierats i samband med väsentlighet- och riskanalysen.

Ledningens genomgång omfattar nedanstående punkter:

- E:utbildning: Informationssäkerhet för medarbetare i staden
- E:utbildning: Grundkurs i dataskydd
- Implementering av lokal anvisning för informationssäkerhet (obligatorisk arbetssätt i väsentlighets- och riskanalysen)
- Informationsklassning (obligatoriskt arbetssätt i väsentlighets- och riskanalysen)
- Riskanalys
- Konsekvensbedömning
- Behörighetshantering (obligatoriskt arbetssätt i väsentlighets- och riskanalysen)
- Registerförteckning personuppgiftsbehandling
- Informationssäkerhet inom upphandlingsförfarandet (obligatoriskt arbetssätt i väsentlighets- och riskanalysen)
- Personuppgiftsbiträdesavtal
- Incidenthantering
- Rapporteringsskyldighet GDPR
- Rapporteringsskyldighet NIS

2.1 Uppföljning 2023

Under året har en arbetsgrupp arbetat med att ta fram lokal anvisning för informationssäkerhet. Informationsklassningar har genomförts med fokus på hantering av känslig information.
De obligatoriska utbildningarna i informationssäkerhet och dataskydd har blivit certifierande.

I stadsdelsförvaltningens tertialrapport 2 2023 rapporterades inga avvikelser. Arbetet bedöms fortlöpa enligt plan.

Risker som identifierats i GDPR-årsrapport
Dataskyddsombudet har i årsrapporten för 2023 föreslagit åtgärder för att säkerställa incidentrapportering.

3 Utveckling av lokalt informationssäkerhetsarbete och dataskyddsarbete

3.1 Verksamhetsplan 2024

Prioriterade områden:

- Implementera lokal anvisning för informationssäkerhet.
- Utse objektledare för samtliga system
- Tillse att informationstillgångar är klassade och att handlingsplaner från klassning tas om hand
- Informationssäkerhet i Risk- och sårbarhetsanalysen
- Utveckla arbetet med incidenthantering.
- Medarbetare: genomgå obligatorisk utbildning i dataskydd och informationssäkerhet.